



DEPARTMENT OF HOMELAND SECURITY

[Docket No. FEMA-2020-0032]

Privacy Act of 1974; System of Records

AGENCY: Federal Emergency Management Agency, U.S. Department of Homeland Security.

ACTION: Notice of New Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, “DHS/Federal Emergency Management Agency (FEMA)-015 Fraud Investigations System of Records.” This system of records allows DHS/FEMA to collect and maintain records on individuals who are being investigated for or involved in an investigation relating to the misuse of federal disaster funds and/or benefits. This system of records further assists FEMA’s Fraud Investigations and Inspections Division (FIID) recordkeeping; tracking and managing fraud inquiries, investigative referrals, and law enforcement requests; and case determinations involving disaster funds and/or benefits fraud, criminal activity, public safety, and national security concerns. Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the *Federal Register*.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective upon publication. New or modified routine uses will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number FEMA-2020-0032 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: James Holzer, Acting Chief Privacy Officer, Privacy Office, U.S.

Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number FEMA-2020-0032. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact:

Tammi Hines, (202) 212-5100, FEMA-Privacy@fema.dhs.gov, Senior Director for Information Management, Federal Emergency Management Agency, Washington, D.C. 20472-0001. For privacy questions, please contact: James Holzer, (202) 343-1717, Privacy@hq.dhs.gov, Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

The U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) proposes to establish a new DHS system of records titled, “DHS/FEMA-015 Fraud Investigations System of Records.” FEMA’s Fraud Investigations and Inspections Division (FIID) is responsible for investigating allegations of fraud involving federal disaster funds and/or benefits by a disaster applicant or contractor associated with a disaster assistance award or grant. These investigations may relate to applicants for FEMA disaster benefits; FEMA employees and contractors who violate law, policy, or procedure; and insurance procurement and grant fraud. FEMA

conducts these investigations pursuant to an inquiry or tip from various sources, including FEMA employees; government contractors supporting FEMA operations; the DHS Office of the Inspector General (OIG); members of the public; and other federal, state, local, or tribal law enforcement entities.

FEMA FIID routinely collects these records as part of standard investigative protocols in support of disaster fraud investigations. In the past few years, FEMA has experienced substantial increases in the amount of fraud involving federal disaster benefits. For example, during the storm events of 2017, FEMA experienced over \$10 million in identity theft fraud which involved stolen personally identifiable information (PII) from both eligible and non-eligible disaster applicants. FEMA has been proactive in working with its federal, state, and local law enforcement partners, including the Federal Bureau of Investigation (FBI), DHS/OIG, U.S. Department of Housing and Urban Development/OIG, U.S. Small Business Administration/OIG, and U.S. Social Security Administration/OIG, in combating and strengthening safeguards to prevent fraud, while also considering the emergency needs of many disaster applicants in the hardest hit areas of the country.

As part of an investigation, FEMA FIID collects PII of disaster applicants from the FEMA National Emergency Management Information System (NEMIS) – Individual Assistance (IA) module. FEMA FIID may also collect or confirm PII from commercial or government databases to include Lexis Nexis, Thomas Reuters CLEAR, National Insurance Crime Bureau / ISO Claim Search Plates, CarFax, or the FBI National Crime Information Center (NCIC). FIID uses the information to document financial transactions and compare data and information located in the different databases to identify indications that may substantiate or disprove fraud by a disaster applicant.

Consistent with DHS's information sharing mission, information collected by FEMA FIID and stored in the DHS/FEMA-Investigative Records System of Records may

be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. FEMA FIID generally shares the information with the Department of Justice, U.S. Attorney Offices; and the U.S. Treasury Department, Bureau of Fiscal Services in accordance with approved Information Sharing and Access Agreements (ISAA). In addition, DHS/FEMA may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in the system of records notice.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the Federal Register. This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/FEMA-015 Fraud Investigations System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA)-015 Fraud Investigations System of Records.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained on access-controlled servers or in access-controlled cabinets that are under the management and control by the FEMA Office of Chief Information Officer at FEMA Headquarters in Washington, D.C., and field offices.

SYSTEM MANAGER(S): FEMA Investigations and Inspections Division (FIID), Fraud Prevention Investigations Branch (FPIB), Fraud Investigations Operations Manager, 400 C Street, SW, Washington, D.C., Suite 7SW-1009, Mail Stop 3005.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Robert T. Stafford Disaster Relief and Emergency Assistance Act, *as amended*, 42 U.S.C. secs. 5161 and 5174(i), as delegated to the Administrator of FEMA in 44 C.F.R. Part 206; The Homeland Security Act of 2002, 6 U.S.C. secs. 793 and 795; and Executive Order 13520, Reducing Improper Payments (2009).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect, maintain, and share records related to fraud investigations conducted by the FEMA FIID. It allows FEMA to conduct the necessary investigations to safeguard and protect federal disaster funds and/or benefits from fraud against the United States.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include any: (1) individual who files a complaint or

report alleging fraud or misuse of federal disaster benefits; (2) individual who is the subject of the disaster fraud complaint or report; (3) individual who has submitted potentially fraudulent applications for disaster fund benefits; and (4) individual who is associated with the fraud investigation but not the actual subject of the investigation and whose information is relevant to the fraud case.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Full name of applicant and co-applicant, including aliases;
- Full names of dependents and/or others living in the dwelling associated with the investigation;
- Full names and addresses of associates and relatives;
- Position or title of applicant or associates and relatives, as needed;
- Date of birth;
- Social Security number (SSN);
- Phone numbers;
- Email addresses;
- Addresses (mailing and damaged dwelling associated with the investigation);
- Address history (addresses lived at prior to the damaged dwelling associated with the investigation);
- Employment information and data (e.g., name of employer, location, job title);
- Banking name and account information, including routing numbers, electronic funds transfer information, and credit/debit account information;
- FEMA Registration Identification Number;
- Property, building, and structural photographs;
- Publicly available criminal records;

- Publicly available civil court records (e.g., bankruptcy, liens, divorce, child custody judgements);
- Driver's license data (current and historical);
- Vehicle records (current and historical);
- Business and professional license information (e.g., Medical Doctor, Certified Public Accountant, Registered Nurse);
- Social media information, to include posts, user name/handles, comments, and photographs;
- National Flood Insurance Program (NFIP) records;
- Private house, property, and vehicle insurance records;
- Voter registration records (to determine location data);
- Property records (e.g., deeds, liens, tax assessments, tax bills, leases, rental receipts, landlord letters and information);
- School or education institution location information (no transcripts or education records);
- Utility Company information;
- Aerial property photographs and Google Earth Street View photographs;
- Transcripts of conversations with FEMA call centers or helpdesk, including name, address, phone number, email address, caller type (e.g., property owner, lessee), chat subject, and chat subject category;
- Other relevant information or documents voluntarily provided by disaster applicants that is contained in the NEMIS database; and
- Names and contact information of complainants and witnesses interviewed by Investigators.

RECORD SOURCE CATEGORIES: Records are obtained from individuals who are the subject of the investigation or inquiry, employers, law enforcement organizations,

members of the public, witnesses, educational institutions, government agencies, nongovernmental organizations, credit bureaus, commercial databases, references, confidential sources, personal interviews, photographic images, financial institutions, and the personnel history and application forms of agency applicants, employees, or contractors.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agencies conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the federal government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.

G. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

H. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order,

when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. To appropriate federal, state, tribal, and local government agencies that provide assistance with disaster fraud investigations for FEMA to investigate and verify the identity of a subject or witness, or investigate and verify the information provided by the subject or witness to the extent disclosure is necessary to obtain information pertinent to the fraud investigation, including those investigations to prevent or identify fraudulent disaster applications involving identity theft.

J. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/FEMA stores records in this system electronically, paper files, magnetic disc, tape, or other digital media in a locked drawer within secure access-controlled facilities.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by an individual's name or address, fraud complaint or investigation number, FEMA Registration Identification Number, or FEMA FIID investigator's name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: In accordance with National Archives and Records Administration (NARA) authority N1-311-99-6, Item 1, AUD 1-1, FEMA FIID retains investigative case files

containing information or allegations which are of an investigative nature but do not relate to a specific investigation for five (5) years. Further, in accordance with NARA authority N1-311-99-6, Item 2, AUD 1-2, FEMA FIID retains all other investigative case files except those that are unusually significant for documenting major criminal or ethical violations by others for ten (10) years from the end of the fiscal year when a case is closed. Additionally, in accordance with NARA authority N1-311-99-6, Item 3, AUD 1-3, FEMA FIID retains significant investigative case files that attract significant attention from the media or Congress; result in substantive agency policies and procedures; or are cited in OIG's periodic reports to Congress. These case files are retired to the Federal Records Center five (5) years from when a case is closed and transferred to the National Archives twenty (20) years from when a case is closed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/FEMA safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies.

DHS/FEMA FIID has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system or any paper files in the access-controlled cabinets are limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable to protect information relating to DHS activities from disclosure to subjects or others related to these activities.

Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; ensure DHS's ability to obtain information from third parties and other sources; and to protect the

privacy of third parties. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

However, DHS/FEMA will consider individual requests to determine whether information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and FEMA FOIA Officer whose contact information can be found at <http://www.dhs.gov/foia> under “Contacts Information.” If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records may be available under the Freedom of Information Act.

When seeking records from this system of records or any other Departmental system of records, the request must conform with the Privacy Act regulations set forth in 6 C.F.R. Part 5. Individuals must first verify identity, meaning that that full name, current address, and date and place of birth must be provided. Request must be signed, and the signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, requestors should:

- Explain why the requestor believes that the Department would have information on the requestor;
- Identify which component(s) of the Department may have the information;
- Specify the records would have been created; and

- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include a statement from that individual certifying his/her agreement for the requestor to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record. For records covered by the Privacy Act or covered Judicial Redress Act records, see “Record Access Procedures” above.

NOTIFICATION PROCEDURES: See “Record Access Procedures” above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. secs. 552a(c)(3); (d); (e)(1); (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). While investigating a complaint, records, or information covered by other systems of records may become part of, merged with, or recompiled

within this system. To the extent this occurs, DHS will claim the same exemptions for those records that are claimed in the original primary systems from which they originated and claim any additional exemptions set forth here.

History: None.

James Holzer,
Acting Chief Privacy Officer,
U.S. Department of Homeland Security.
[FR Doc. 2021-05645 Filed: 3/19/2021 8:45 am; Publication Date: 3/22/2021]